RSAC 2025 Conference

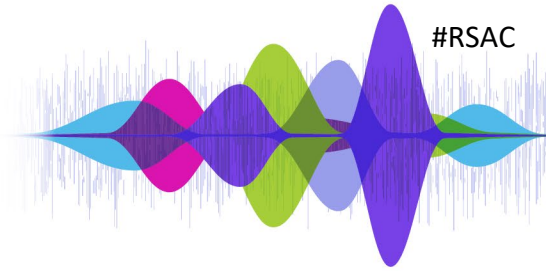
Many Voices.
One Community.

SESSION ID: NCS-M01

Having Zero Trust to Give: What should have been next?

Andy Ellis

Partner
YL Ventures
www.csoandy.com



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Andy Ellis

www.csoandy.com
@csoandy

Partner
YL Ventures

Author
1% Leadership

2021 inductee
CSO Hall of Fame

Podcast Co-host
CISO Series

CEO/Principal
Duha

Former CSO
Akamai

Former Officer
US Air Force

Graduate – CS/Math
MIT

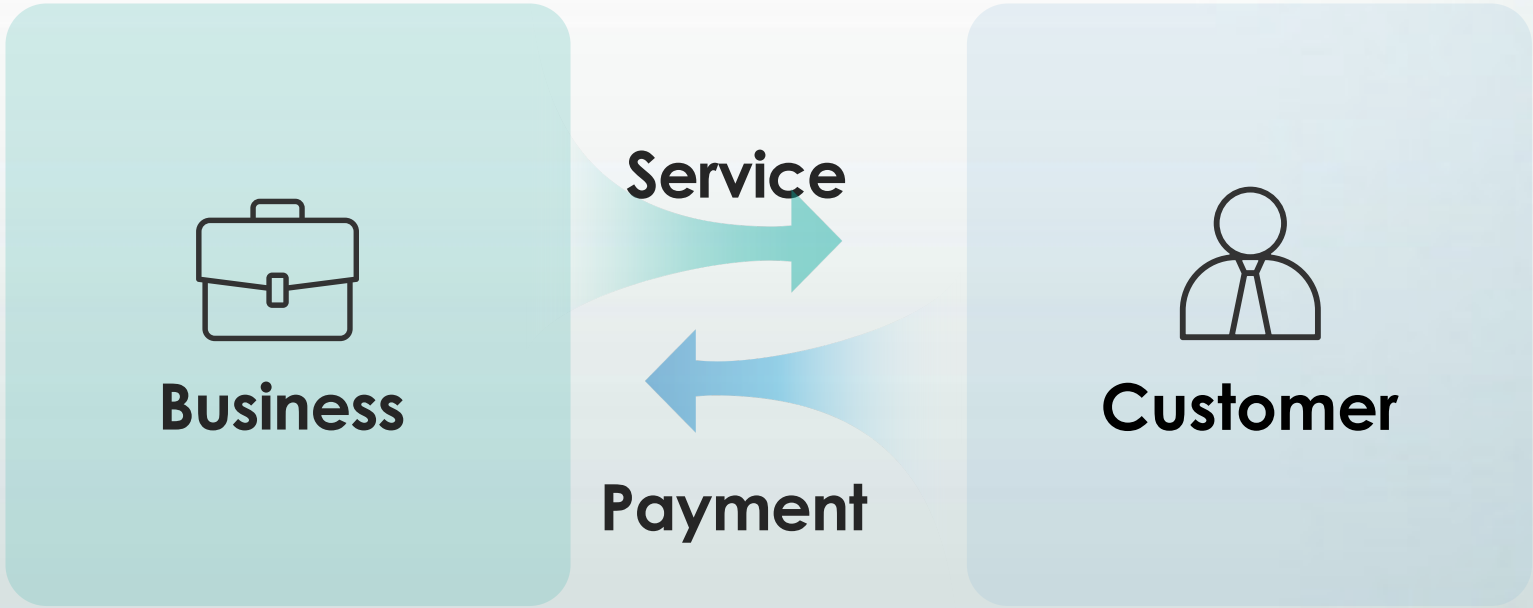
Spirit of Disneyland
Disneyland

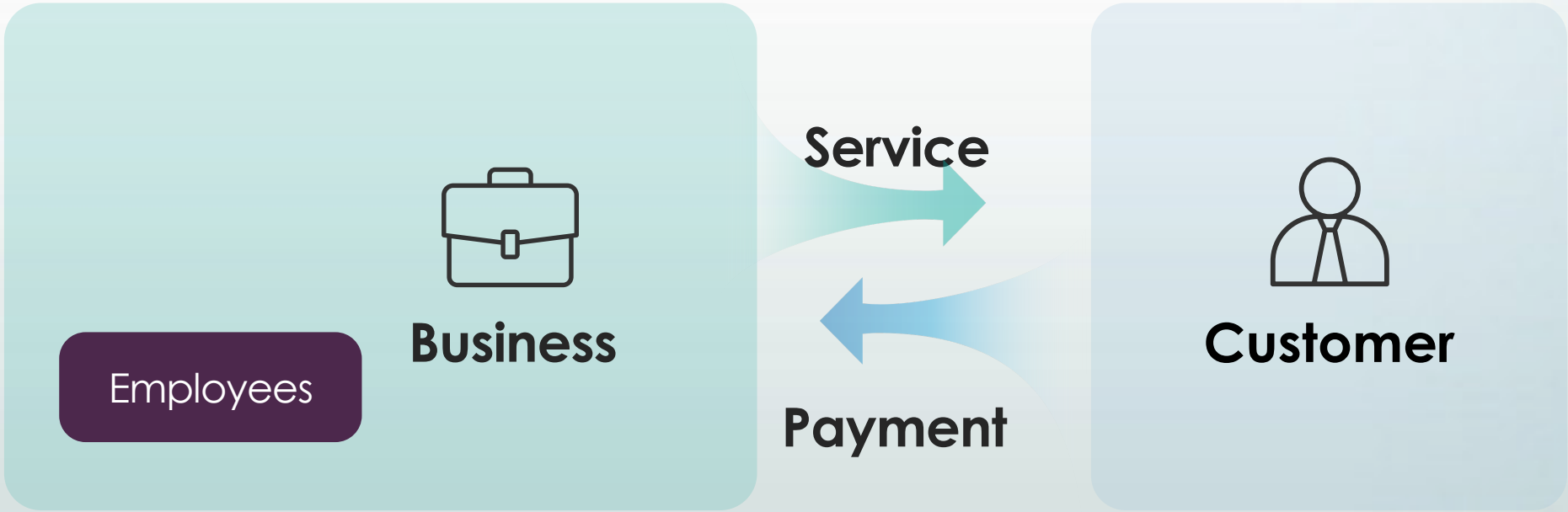
Award of Excellence
Wine Spectator

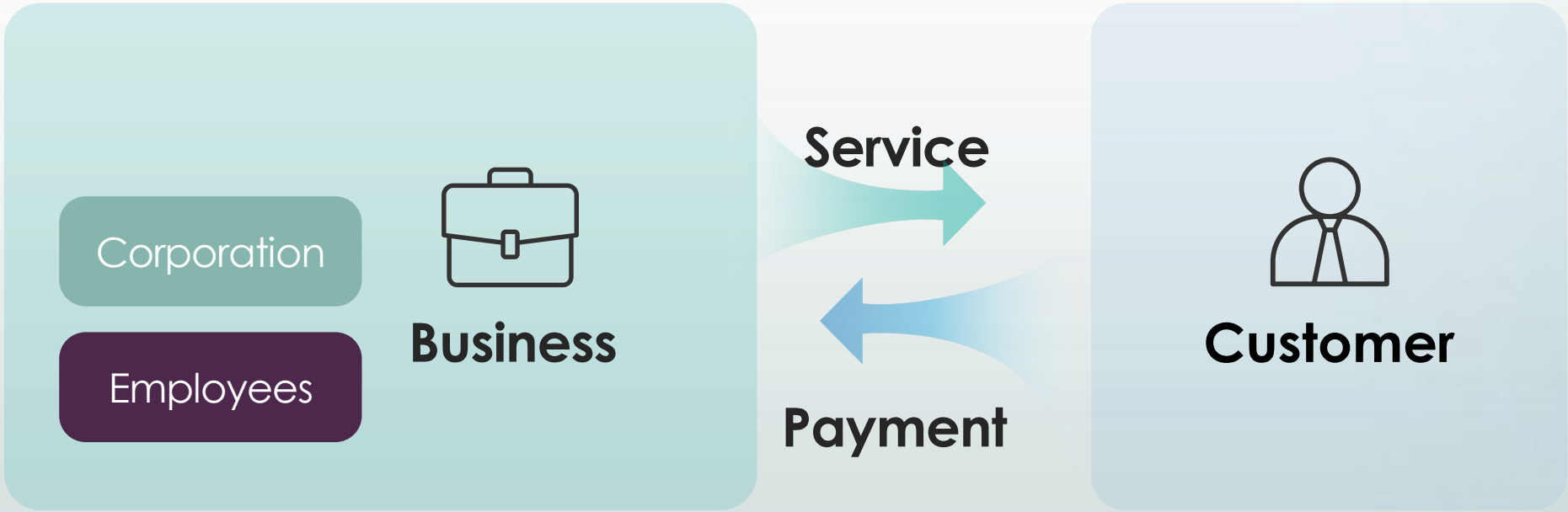
A Brief History of Trust

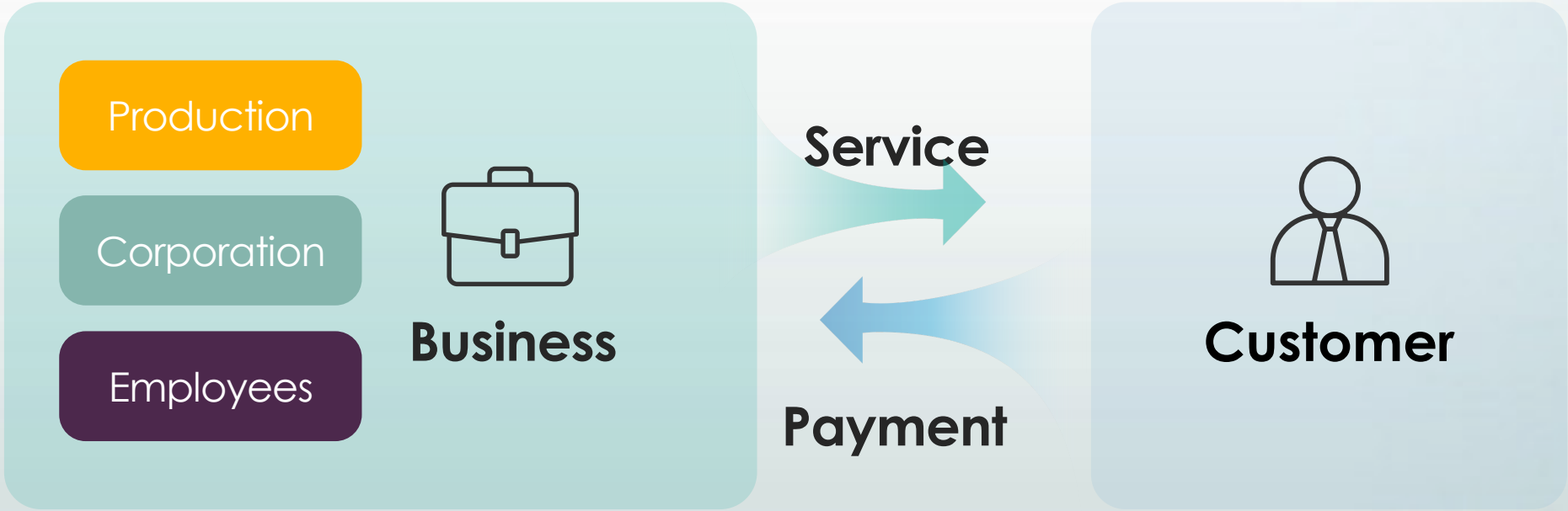
A Brief History of IT

A Brief History of Business


Service
Business
Customer
Payment

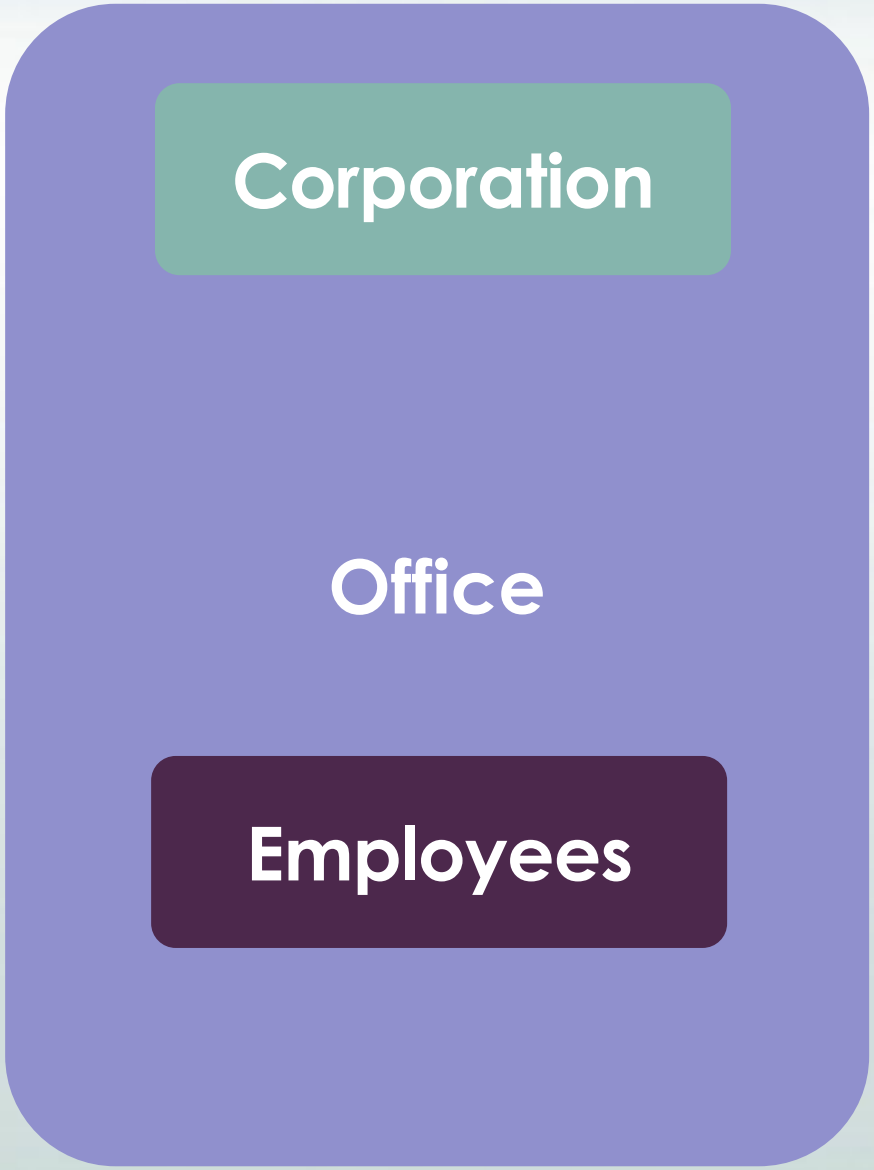

Service
Business
Employees
Payment
Customer


Corporation
Employees
Business
Service
Payment
Customer


Production
Corporation
Employees
Business
Service
Payment
Customer

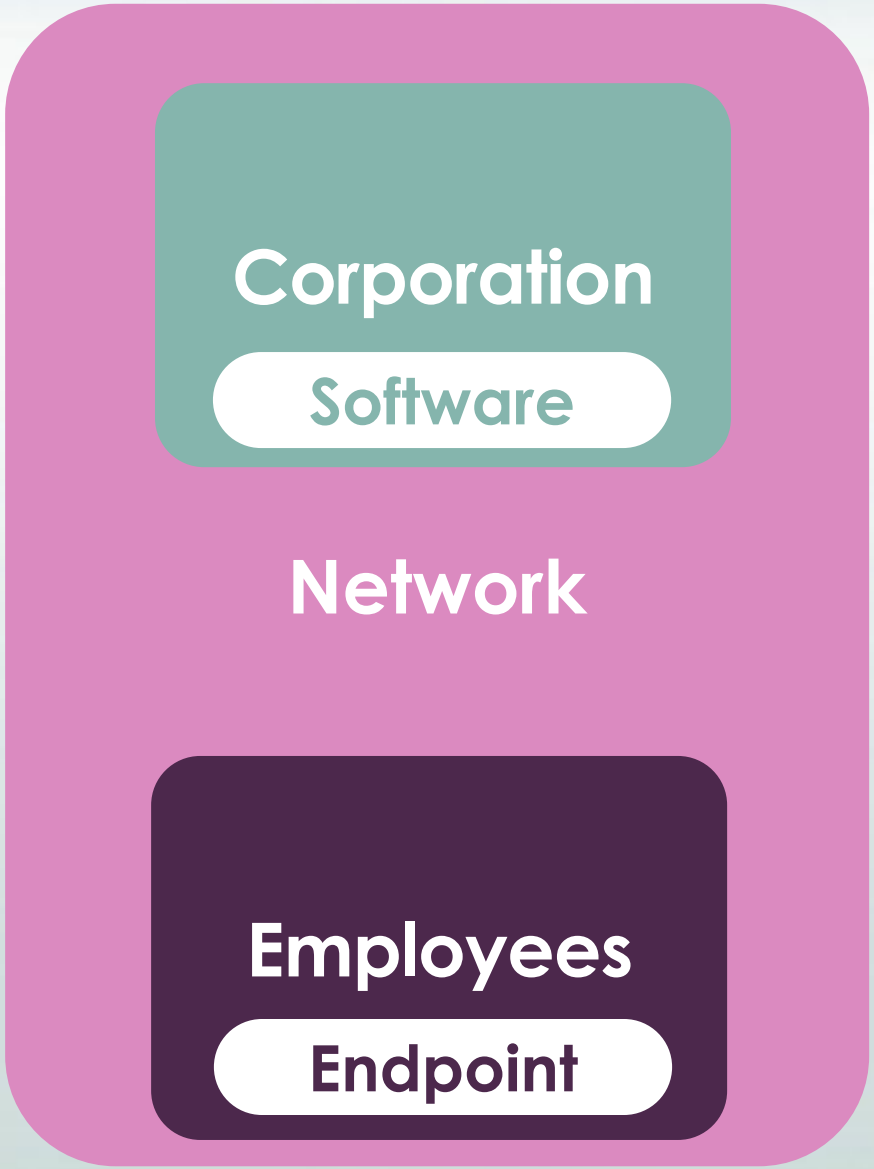
Corporation

Employees

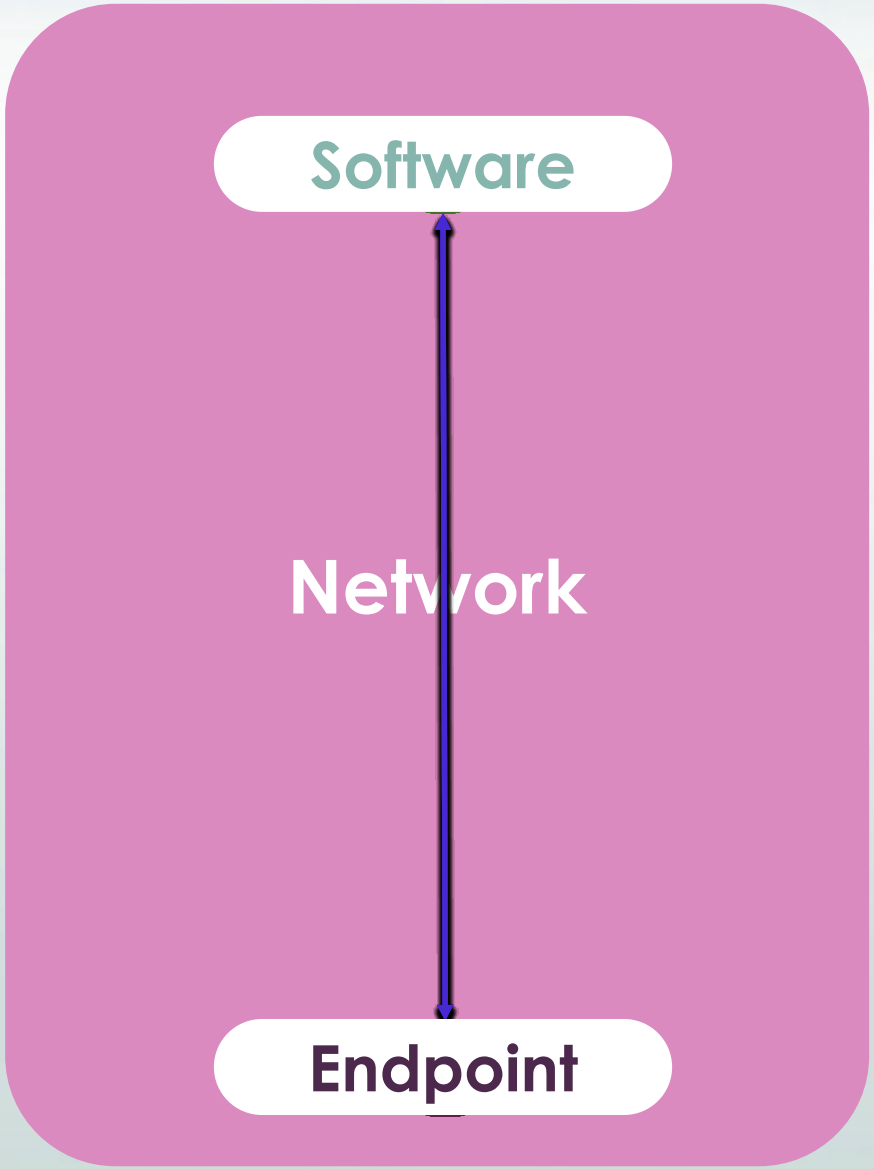

Corporation
Office
Employees

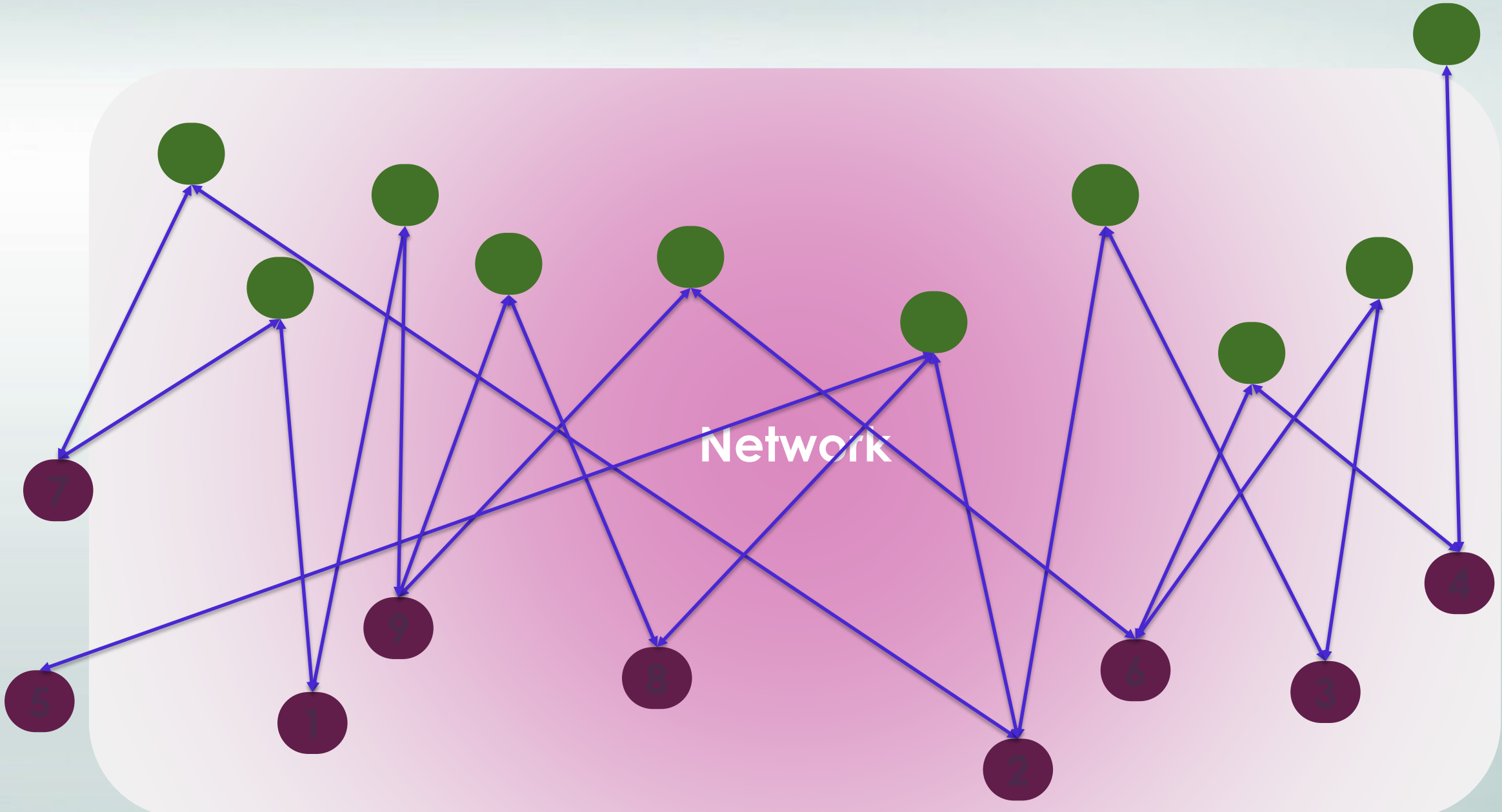
Corporation
Ledgers
Office
Employees
Pencils

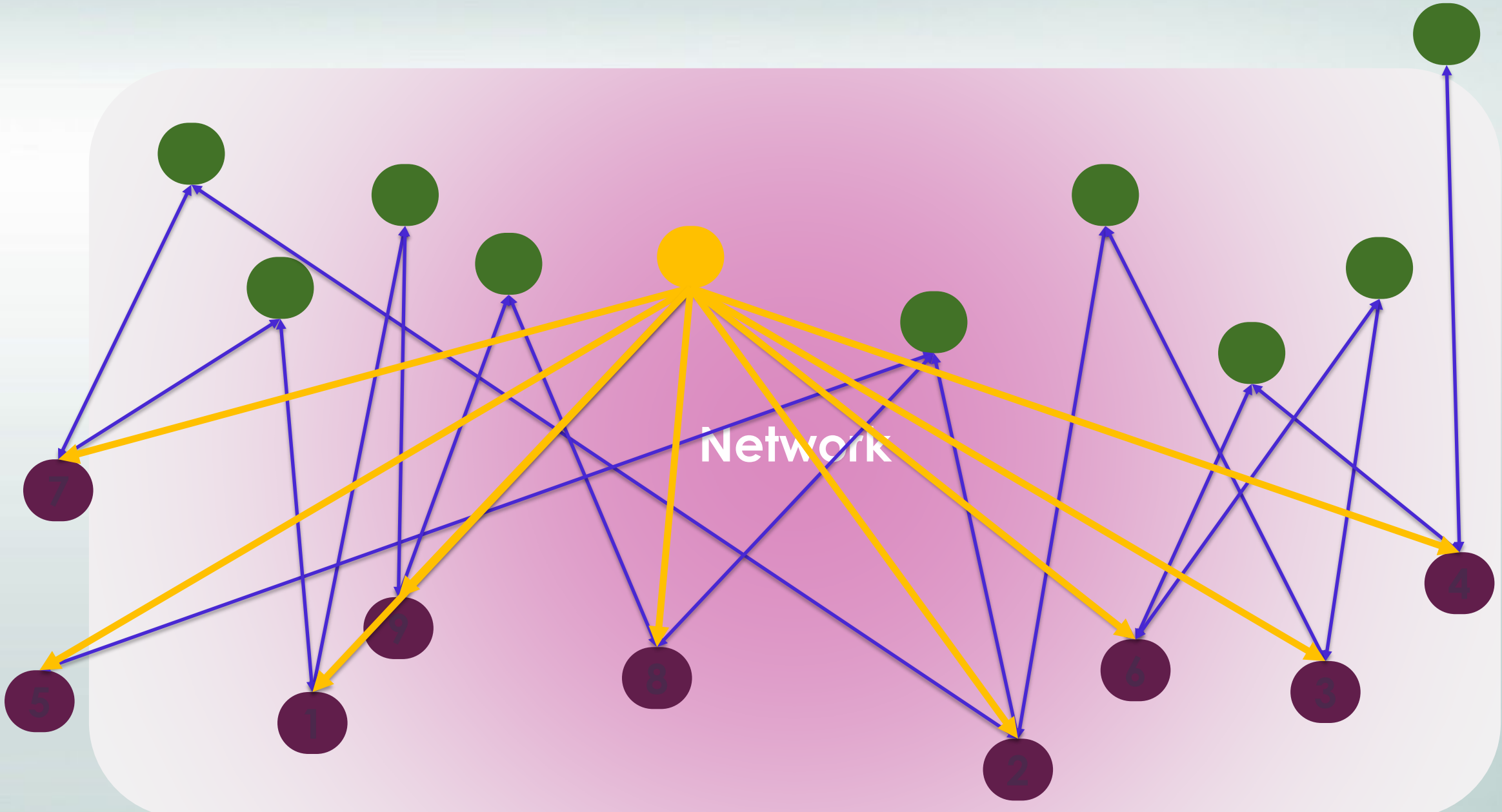
Corporation
Software
Office
Employees
Endpoint

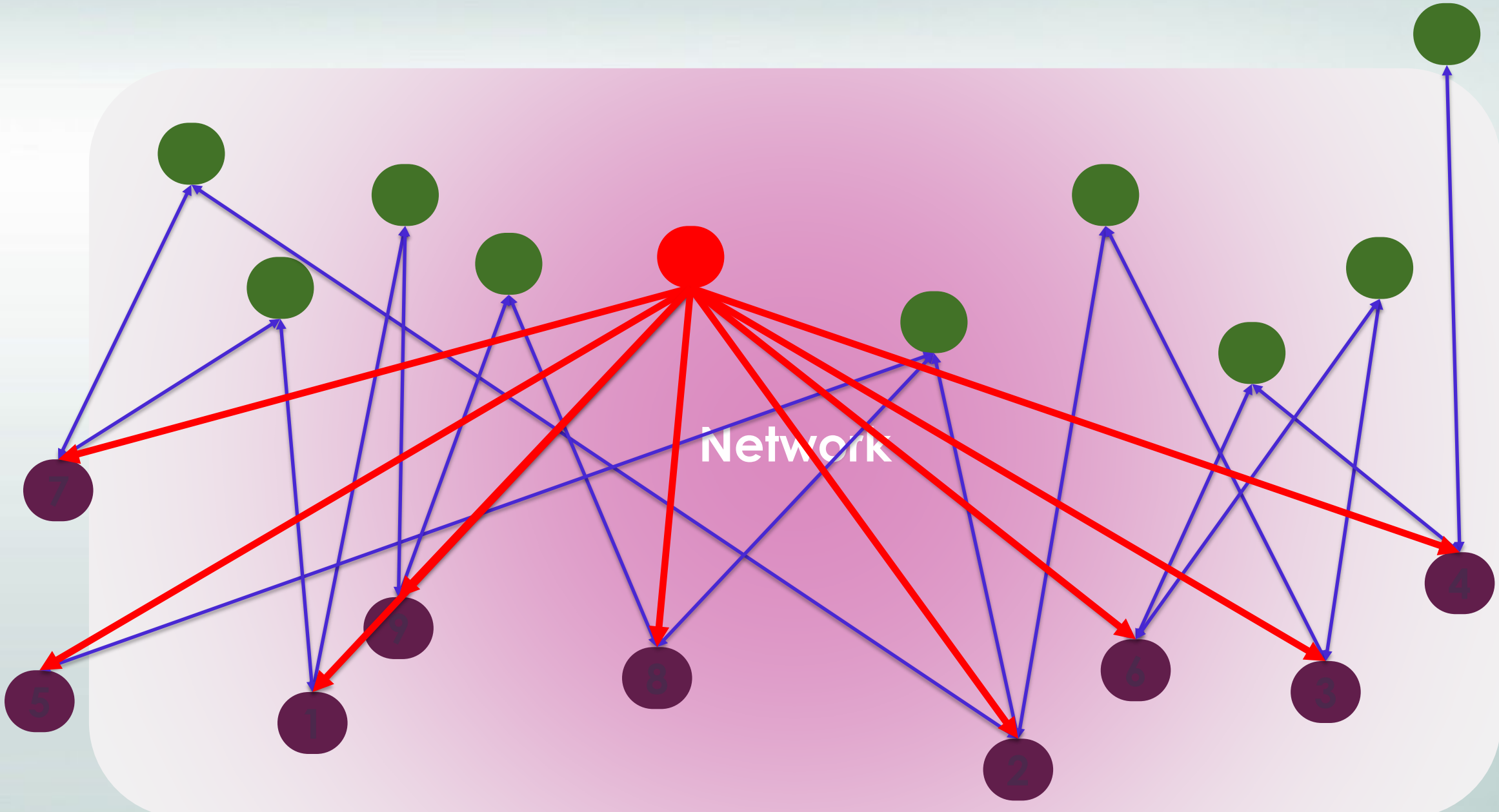

Corporation
Software
Network
Employees
Endpoint

Software
Network
Endpoint


Software
Network
Endpoint


Network
7
9
8
6
3
4
5
1
2


Network
7
9
8
6
5
1
2
3
4


Network
7
9
8
6
5
1
2
3
4

How did we respond?

How did we respond?

Software

Network

We *should* have removed trust on the endpoint

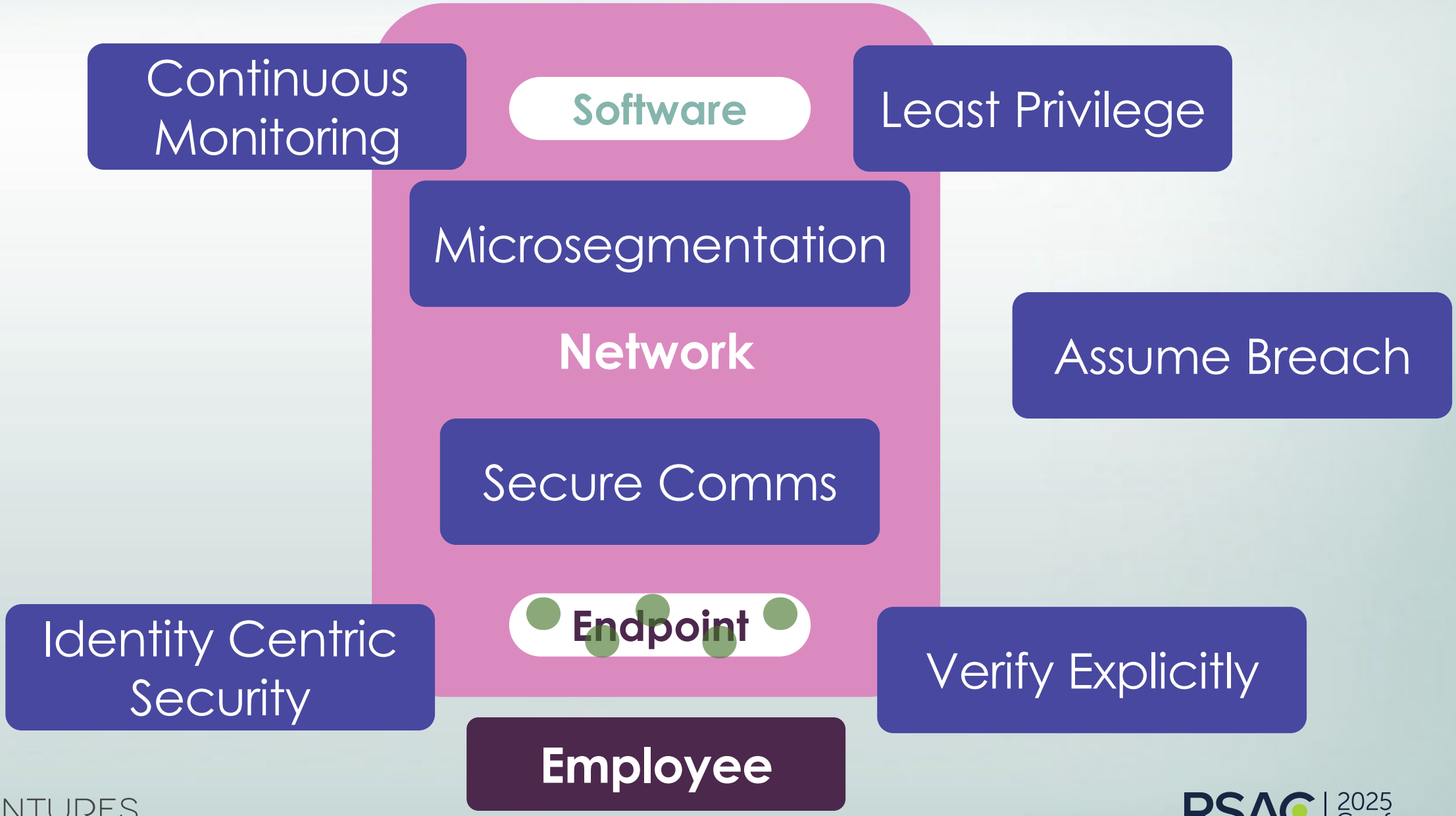
Employee

Endpoint

How did we respond?

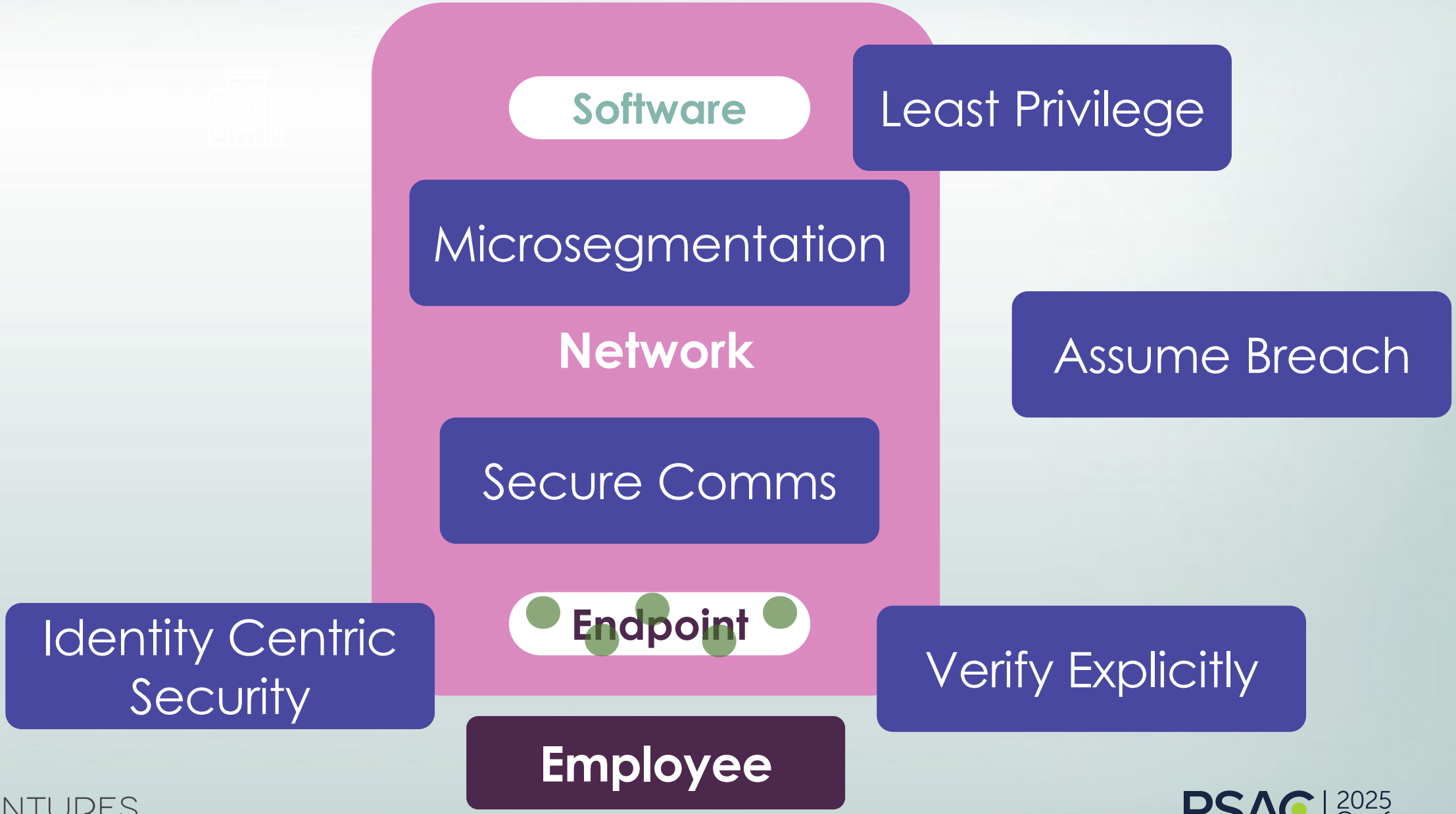
We *should* have removed trust on the endpoint

Instead, we made the endpoint trust *more* software


Continuous Monitoring
Software
Least Privilege
Microsegmentation
Network
Assume Breach
Secure Comms
Identity Centric Security
Endpoint
Verify Explicitly
Employee

Continuous Monitoring

Employee


Software
Least Privilege
Microsegmentation
Network
Assume Breach
Secure Comms
Endpoint
Identity Centric Security
Verify Explicitly
Employee

Assume Breach

Employee

Limited Assumption of Privilege

Identity Centric Security

Endpoint

Verify Explicitly

Employee

Limited Assumption of Privilege

Identity Centric Security

Endpoint

Employee

Verify Explicitly

Limited Assumption of Privilege

Identity Centric Security

Endpoint

Employee

Limited Assumption of Privilege

Software

Least Privilege

Microsegmentation

Network

Secure Comms

Identity Centric Security

Endpoint

Employee

Limited Assumption of Privilege

Software

Least Privilege

Microsegmentation

Network

Secure Comms

Identity Centric Security

Endpoint

Employee

Limited Assumption of Privilege

Individualized, strong authentication

Software

Least Privilege

Microsegmentation

Network

Endpoint

Employee

Limited Assumption of Privilege

Individualized, strong authentication

SaaS / Cloud

Software

Least Privilege

Network

Microsegmentation

Endpoint

Employee

Network

Network

Limited Assumption of Privilege

Individualized, strong authentication

SaaS / Cloud

Software

Least Privilege

Endpoint

Employee

Limited Assumption of Privilege

Individualized, strong authentication

Minimize unused privilege

SaaS / Cloud

Software

Endpoint

Employee

Limited Assumption of Privilege

Individualized, strong authentication

Minimize unused privilege

Limited Assumption of Privilege

Reduce/Eliminate Admin

Non-copyable access tokens

Individualized, strong authentication

Minimize unused privilege

Limited Assumption of Privilege

Reduce/Eliminate Admin

Non-copyable access tokens

Individualized, strong authentication

Endpoint is part of the User

Cryptographically strong auth

Minimize unused privilege

Limited Assumption of Privilege	Reduce/Eliminate Admin
	Non-copyable access tokens
Individualized, strong authentication	Endpoint is part of the User
	Cryptographically strong auth
Minimize unused privilege	Separate *Authorization & Grant*
	Streamline grant provisioning

Limited Assumption of Privilege	Reduce/Eliminate Admin
	Non-copyable access tokens
Individualized, strong authentication	Endpoint is part of the User
	Cryptographically strong auth
Minimize unused privilege	Separate *Authorization* & *Grant*
	Streamline grant provisioning

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

Rethink Your Architecture

Take Baby Steps

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

Rethink Your Architecture

- Stop trusting admin tools
- Phish-proof authentication
- Enable authorization without grants

Take Baby Steps

APPLY

- Limited Assumption of Privilege
- Individualized, strong authentication
- Minimize unused privilege

Rethink Your Architecture

- Stop trusting admin tools
- Phish-proof authentication
- Enable authorization without grants

Take Baby Steps

- Find duplicate credentials
- Tie authentication to the endpoint
- Make provisioning easy

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You

Talk webpage →